

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

JAMES BONCZEK,

Defendant.

08 CRIM 361 (PAC)

AFFIDAVIT OF MICHAEL G. KESSLER IN SUPPORT OF
DEFENDANT'S MOTION FOR FORENSIC REVIEW OF
COMPUTER EVIDENCE

STATE OF NEW YORK)
 : SS.:
COUNTY OF NEW YORK)

MICHAEL G. KESSLER, being duly sworn, states as follows:

1. I am president and CEO of Kessler International, a firm specializing in computer forensic investigation.
2. Prior to founding Kessler International, I was Chief of Investigations for N.Y.S. Tax and Finance, Director for the N.Y.S. Revenue Crimes Bureau, Deputy Inspector General for the N.Y. Metropolitan Transportation Authority, and Assistant Chief Auditor/Investigator for the N.Y.S. Special Prosecutor.
3. I have been retained by the defendant in the above-captioned case to perform forensic investigation of the computers seized from his apartment

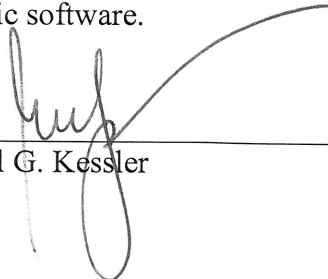
on October 18, 2007. It is my understanding that the defendant may seek to present my expert testimony at trial.

4. I have attempted to examine the seized computers to determine, among other things, every action performed on and by the computers on October 17 and 18, 2007, including which computer files were opened and/or searched, which images were shown, how long the screensaver was active, was it reactivated at any time on the evening of October 17, and at what particular times.
5. All of the seized computers are manufactured by Apple, and use the Macintosh operating system.
6. Pursuant to the June 26, 2008 stipulation between Ms. Necheles and the government, I commenced an examination of the computers using a government-provided Windows-based computer running Access Data's Forensic Toolkit software ("FTK").
7. The examination was unsuccessful because it is not possible to perform a comprehensive forensic analysis of Macintosh computers using a Windows-based computer and Windows-based FTK software.
8. A proper forensic analysis would include "mounting" the data from the seized Macintosh hard drives as a virtual machine, thus emulating the data in its native setting. It is then possible to answer questions such as those posed in paragraph #4 above. Due to fundamental differences between the Windows and Macintosh operating systems, however, it is impossible to

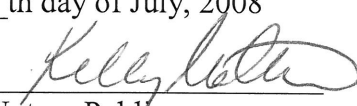
mount the Macintosh data using a Windows-based computer and Windows-based FTK software.

9. The most important difference involves the method used to store data in files. The Macintosh operating system uses two “forks” to store data in files: a resource fork and a data fork. The Windows-based operating system does not support the resource fork. Due to this incompatibility, forensic review of Macintosh computers on a Windows-based computer will be incomplete and inaccurate.
10. An additional incompatibility problem is the inability to parse Macintosh “.DMG” files using a Windows-based forensic system operating FTK. Due to this limitation, items deleted from the Macintosh drives may not be found by examination using a Windows-based forensic system.
11. Using Windows-based forensic tools to examine Macintosh data would present that data outside of its original environment, such that crucial context and meaning would be lost in translation. Due to the incompatibilities between the systems, it would be impossible to learn exactly what actions were performed by and on the seized Macintosh computers on October 17 and 18, 2007.
12. Proper forensic protocol is that the forensic examination of a Macintosh computer be performed using a Macintosh computer with Macintosh-based forensic software.

13. To perform the analysis as directed by defense counsel, I must review the evidence using a Macintosh-based computer with Macintosh-based forensic software.
14. I could perform the necessary analysis either with my own Macintosh computer or with a government-provided Macintosh computer running Macintosh-based forensic software that I would identify to the government.
15. Based on my review of the forensic computer files produced by the government, it appears that the government has reviewed the evidence using Macintosh computers and Macintosh-based forensic software. It is my understanding, therefore, that the government has access to Macintosh computers and Macintosh-based forensic software.



Michael G. Kessler

Sworn to before me this
14th day of July, 2008


Notary Public

KELLY MATTMULLER
Notary Public - State of New York
No. 01MA6104672
Qualified in Suffolk County
Commission Expires Jan. 26, 2008/2